ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑAR MEJORAS EN LA SEGURIDAD DE LA RED DE DATOS EN UNA EMPRESA DE DESARROLLO DE SOFTWARE UTILIZANDO TÉCNICAS DE HACKING ÉTICO Y PRUEBAS DE PENETRACIÓN”

TESIS DE GRADO

Previa a la obtención de título de

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. STEWART CHRISTIAN PULLEY PESANTES

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Agradezco a mi familia por su apoyo incondicional y comprensión durante este arduo proceso.

Ing. Christian Pulley Pesantes

DEDICATORIA

Dedico este logro académico a varias personas que han sido mí inspiración mi madre y mi abuela quienes me enseñaron la importancia del esfuerzo y la perseverancia, mi esposa quien junto a mis hijos son la fuente de mí fortaleza y apoyo incondicional para llegar al objetivo.

Ing. Christian Pulley Pesantes

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Freire Cobo

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

Mgs. Juan Carlos García

REVISOR

DECLARACIÓN EXPRESA

Yo Stewart Christian Pulley Pesantes acuerdo y reconozco que: La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores. El o los estudiantes deberán procurar en cualquier caso de cesión de sus derechos patrimoniales incluir una cláusula en la cesión que proteja la vigencia de la licencia aquí concedida a la ESPOL.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, secreto empresarial, derechos patrimoniales de autor sobre software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí durante el desarrollo del

proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al autor que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 12 de noviembre del 2024.

Firmado electrónicamente por:
STEWART CHRISTIAN PULLEY PESANTES

Ing. Christian Pulley Pesantes

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Freire Cobo

PROFESOR TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

Mgs. Juan Carlos García

PROFESOR EVALUADOR

RESUMEN

Este trabajo de titulación está enfocado en diseñar mejoras significativas en la seguridad de la red de datos de una empresa especializada en desarrollo de software. El objetivo fundamental consiste en la aplicación de técnicas de hacking ético y pruebas de penetración como estrategias proactivas para identificar, evaluar y abordar posibles vulnerabilidades y brechas de seguridad en la infraestructura de red de datos de la empresa.

En un entorno digital donde la información es un activo crítico, la necesidad de salvaguardar la confidencialidad, integridad y disponibilidad de los datos es una prioridad para cualquier organización de tal manera que la continuidad de la operación no se vea comprometida ante cualquier evento de seguridad informática. En este proceso no solo se busca asegurar la protección de la información sensible, sino también mejorar la respuesta y tiempos de recuperación de la empresa ante posibles amenazas ciberneticas.

A través de un análisis de la arquitectura de la red de datos, se identificarán posibles brechas y puntos vulnerables los cuales se evaluarán a detalle, las técnicas de hacking ético y las pruebas de penetración se utilizarán de manera ética y controlada para simular escenarios realistas de amenazas.

Los resultados de estas pruebas servirán como base para el diseño de recomendaciones como medidas correctivas y preventivas.

ÍNDICE GENERAL

ABREVIATURAS

PWC	Plataforma web colaborativa
ISP	Proveedor de servicios de internet
APT	Amenaza persistente avanzada
BD	Base de datos
DDOS	Denegación de servicio distribuida
HW	Hardware
IDS	Sistema de detección de intrusos
MFA	Autenticación Multifactor
PWC	Plataforma web colaborativa
SIEM	Gestión de información y eventos de seguridad
SW	Software
VPN	Red privada virtual

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la era digital actual, la seguridad informática es una preocupación crítica para las empresas de desarrollo de software, que manejan grandes cantidades de datos sensibles y confidenciales. Los ciberataques se han vuelto cada vez más sofisticados y frecuentes, poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información empresarial. A pesar del creciente reconocimiento de la importancia de la seguridad informática, muchas empresas de desarrollo de software carecen de un enfoque estructurado para evaluar y mejorar su postura de seguridad. La falta de recursos adecuados y la escasez de personal capacitado en técnicas avanzadas de seguridad aumentan el riesgo de brechas de seguridad. Sin un plan de acción claro y bien definido, las organizaciones se enfrentan a la posibilidad de sufrir daños significativos tanto en términos financieros como de reputación.

El objetivo principal de esta tesis es desarrollar un plan de acción integral para mejorar la seguridad de la red de datos en una empresa de desarrollo de software, utilizando técnicas de hacking ético y pruebas de penetración. Este enfoque sistemático no solo busca identificar y mitigar las vulnerabilidades presentes, sino también establecer procedimientos de monitoreo y auditoría continua para asegurar la efectividad de las

medidas de seguridad implementadas. Además, se pretende crear un plan de capacitación para el personal en prácticas de seguridad informática, promoviendo una cultura de seguridad dentro de la organización. La implementación de este plan de acción no solo protegerá los activos críticos de la empresa, sino que también asegurará el cumplimiento normativo y mejorará la confianza de los clientes y socios comerciales

CAPÍTULO I

GENERALIDADES

1.1 Antecedentes

La empresa de desarrollo de software es una compañía multinacional la cual mantiene oficinas en Ecuador, Colombia, Alemania, Suiza y Estados Unidos, cuenta con más de 25 años de experiencia en el campo tecnológico, brindando soluciones de software personalizadas a cualquier industria sea esta pequeña, mediana o grande, la empresa suministra productos y servicios a más de 10.000 usuarios en más de 20 países.

En Ecuador la oficina de la empresa está ubicada en la ciudad de Guayaquil donde cuenta con una nómina menor a 50 colaboradores gran parte de esta nómina se dedica al desarrollo de las soluciones informáticas manteniendo conectividad con servidores ubicados en su oficina sede situada en Alemania.

El autor [1] menciona qué el creciente uso del internet y la dependencia de la tecnología e infraestructuras aumentan la vulnerabilidad tanto en el número posible de ciberataques como en el origen del ataque, poniendo en riesgo la seguridad de los datos almacenados, muchas de las fallas existentes hoy en día son causadas en gran parte por el comportamiento humano, especialmente por la poca importancia o carencia de conocimientos sobre procedimientos y configuraciones de los sistemas.

La operación de la empresa está directamente relacionada a la intercomunicación con servidores ubicados en Europa, este escenario mantiene para la empresa una amplia superficie de ataque tomando en cuenta que en la actualidad la empresa de desarrollo de software no cuenta con las contramedidas necesarias para disminuir el riesgo de ser vulnerables en caso de accesos no autorizados.

1.2 Descripción del problema

La empresa donde se realizará el proyecto es una empresa de desarrollo de software que cuenta con 25 colaboradores por lo cual la

infraestructura de red es pequeña, además se tiene el acceso a los datos ya que contamos con la colaboración del coordinador TI de la empresa de desarrollo de software y en base a una planificación detallada y al contar con los accesos se considera factible la realización en el tiempo propuesto de 4 meses.

Respecto a la factibilidad tecnológica se tiene acceso a tecnologías que permiten realizar el análisis de seguridad de manera efectiva de la mano con la autorización para acceder a la red empresarial y cumpliendo las normas legales relacionadas con las pruebas de seguridad se valida la viabilidad para realizar el proyecto.

En la actualidad la empresa opera en un entorno altamente interconectado y dependiente de la tecnología, ya que es parte de una organización con sede en Alemania por lo cual mantiene comunicación con infraestructura tecnológica de la sede principal, en este escenario la seguridad informática se ha convertido en un factor crítico para la protección de activos, la continuidad del negocio y la reputación de la empresa ante los clientes y socios comerciales. A pesar de la implementación de medidas de seguridad, las amenazas informáticas siguen evolucionando, lo que plantea la necesidad de una evaluación continua y proactiva de la seguridad en la red empresarial.

Esta problemática reside en la presencia de posibles vulnerabilidades y

amenazas en la infraestructura de red, sistemas y aplicaciones de la empresa de desarrollo de software, que podrían ser explotadas por agentes maliciosos. Estas vulnerabilidades ponen en riesgo la confidencialidad, la integridad y la disponibilidad de datos críticos, así como la capacidad de la empresa de desarrollo de software para mantener sus operaciones en caso de un ataque informático.

A inicios del año 2020 la empresa de desarrollo de software sufrió un ataque informático el cual afecto la operación de la empresa por aproximadamente 24 horas, se originó mediante la técnica de phishing cuando uno de los colaboradores accedió a un correo malicioso, lo cual comprometió datos del servidor de desarrollo afectando físicamente al disco duro, viéndose en la necesidad de montar un respaldo del día anterior al ataque para recuperar la operación.

La necesidad de una evaluación de seguridad mediante hacking ético y técnicas de penetración se vuelve evidente para identificar y mitigar las vulnerabilidades existentes y así evitar que se conviertan en amenazas reales a fin de minimizar el riesgo y asegurar la continuidad de las operaciones. La empresa de desarrollo de software se encuentra en un proceso de crecimiento abriendo sucursales en otros países de Sudamérica, además está repotenciando sus procesos enfocados en optimizar el resultado de sus proyectos lo cual va de la mano con un plan

de acción para remediar las vulnerabilidades identificadas.

Este proyecto es factible ya que la empresa de desarrollo de software mantiene una infraestructura tecnológica pequeña por la cantidad de colaboradores y la operación que realiza siendo una filial en Ecuador de una transnacional con sede en Alemania, además se tiene el acercamiento ya que contamos con la colaboración de la Gerencia de TI de la empresa de desarrollo de software y la respectiva autorización de la Gerencia General y en base a una planificación detallada se considera factible la realización en el tiempo estimado de 4 meses.

Respecto a la factibilidad tecnológica se tiene el conocimiento de las técnicas y el acceso a las herramientas que permitan realizar el análisis de seguridad de manera efectiva y cumpliendo con las normas legales.

Finalmente, Ecuador en el 2023 se encuentra entre los 3 países con más ataques cibernéticos en la región entre los más comunes se encuentran ataques de “malware”, “ransomware” y “phishing”, lo que pone en evidencia la realidad de las empresas ecuatorianas al no implementar controles tanto preventivos como de respuesta en caso de involucrarse en un ataque informático.

1.3 Solución propuesta

Una vez identificada la problemática de esta propuesta de titulación la

solución que se propone es diseñar un conjunto de acciones como la identificación de vulnerabilidades y brechas de seguridad a través de Ethical hacking y pruebas de penetración con el fin de determinar un plan de contingencia para minimizar las amenazas que sean identificadas.

El autor [1] explica al Ethical hacking como una técnica de gestión de riesgos que implica el uso de habilidades y herramientas de hacking para identificar vulnerabilidades en sistemas informáticos y redes, con el fin de protegerlos contra ataques maliciosos.

Las fases de “Ethical hacking” son el reconocimiento, escaneo y enumeración, acceso, mantener acceso y cubrir huellas.

Entre las técnicas más utilizadas de acuerdo con el autor [2] están las siguientes:

- Recolección de información o reconocimiento.
- Evaluación de vulnerabilidades
- Inyección de “malware”
- Ataques a aplicaciones web, inyección “SQL”

En relación con las técnicas mencionadas y los procesos que se realizaran para la solución planteada se detallan a continuación:

Identificar los activos de información en la infraestructura de red de la empresa. Realizar revisiones de seguridad y pruebas de penetración a la red de datos, con el fin de identificar vulnerabilidades en la infraestructura de red y sistemas operativos que puedan ser corregidas, así como informar a la alta Gerencia y sensibilizar al personal sobre las fallas encontradas y los principios de seguridad informática.

Establecer un programa de gestión de incidentes de seguridad que permita detectar y responder rápidamente a posibles ataques o brechas de seguridad. Esto implica contar con un equipo capacitado y dedicado a la detección, análisis y mitigación de incidentes de seguridad. Además, se debe establecer un sistema de monitoreo continuo y actualización de las medidas de seguridad implementadas, con el fin de garantizar su efectividad a lo largo del tiempo.

Con la aplicación de estas técnicas se busca identificar accesos no autorizados a toda la información sensible y brechas de seguridad con el objetivo de aplicar las correcciones y recomendaciones necesarias para que la empresa de desarrollo de software logre minimizar el riego limitar el acceso a los datos más sensibles que puedan afectar la operación y reputación de esta.

Esta solución permitirá a la empresa tener un panorama bastante claro de su situación actual respecto a la seguridad en los aspectos

mencionados a continuación:

- Identificación de vulnerabilidades
- Pruebas reales
- Cuantificar los riesgos
- Mejorar políticas y procedimientos
- Cumplimiento normativo
- Concientización en seguridad
- Cumplimiento de objetivos empresariales

1.4 Objetivo general

Optimizar la seguridad de la red de datos en una empresa de desarrollo de software mediante la realización de un diseño de seguridad basado en la aplicación de técnicas de hacking ético y pruebas de penetración para identificar y mitigar vulnerabilidades en la infraestructura de red, fortaleciendo la postura de seguridad de la organización.

1.5 Objetivos específicos

- Realizar un inventario de los activos de la información de la red de datos de la empresa.

- Determinar las vulnerabilidades de la infraestructura de red y sistemas operativos.

- Desarrollar un plan de acción para abordar y remediar las vulnerabilidades identificadas.

1.6 Metodología

Este trabajo de titulación es de tipo descriptivo porque mediante el uso de herramientas de exploración externa a la empresa, nos permitirá obtener información del estado actual de las vulnerabilidades que podrían explotarse con objetivos maliciosos y poner en riesgo la integridad de los datos sensibles de la empresa.

Estará basado en un estudio de tipo no experimental con alcance transversal ya que el análisis de los datos como el inventario de activos tecnológicos a evaluar, el personal involucrado en la operación de la empresa son datos que no van a variar durante el análisis a realizar además esta evaluación se realizara en un tiempo definido de acuerdo con la planificación del proyecto.

Se utilizarán a un grupo focal en el que se involucrarán a 10 personas del área de desarrollo y tecnología de la empresa a las cuales se les aplicara 10 preguntas, las cuales estarán vinculadas a lo siguiente:

- Conciencia de seguridad de los colaboradores

- Identificar políticas existentes
- Percepción de riesgos de la alta Gerencia

Esta información nos llevara al análisis de cómo está involucrada la empresa con la seguridad informática y los procesos existentes, identificar aspecto a mejorar o implementar respecto a la seguridad con el objetivo de minimizar riegos y bajar el impacto en caso de un evento de seguridad.

Posteriormente se realizará un inventario de la infraestructura tecnológica con la que opera la empresa de desarrollo de software, información que nos llevará a documentar hardware, software, versión de firmware, versión de aplicaciones, licenciamiento de aplicaciones.

A continuación, se requiere identificar las vulnerabilidades en la infraestructura de red y aplicaciones, información que se obtendrá en base al análisis de la segregación de funciones en la empresa de desarrollo de software, manejo de claves de accesos, manejo de actualizaciones, accesos físicos, identificando tecnología obsoleta.

Finalmente se elaborará un plan de acción o plan de contingencia con las mejoras aplicadas y las recomendaciones que la alta gerencia debe implementar para mitigar los riesgos existentes y asumir el riesgo residual.

CAPÍTULO II

MARCO TEÓRICO

2.1 Seguridad de la información

La seguridad de la información se refiere a la protección de los datos y los sistemas de información contra el acceso no autorizado, el uso, la divulgación, la interrupción, la modificación o la destrucción. Esto incluye la protección de la confidencialidad, integridad y disponibilidad de la información, de acuerdo al autor [3]

Por su parte el autor [4] nos menciona que la seguridad de la información se refiere a la protección de la información y los sistemas que la almacenan, la seguridad de la información se logra mediante la implementación de medidas técnicas, administrativas y físicas para proteger la confidencialidad, integridad

y disponibilidad de la información.

Podemos agregar según lo indicado por el autor [4] que la seguridad de la información es esencial para garantizar la privacidad de los datos personales, la protección de la propiedad intelectual y la continuidad del negocio. Además, se indica que la seguridad de la información es necesaria para proteger la confidencialidad, integridad y disponibilidad de la información.

En general, los objetivos de seguridad de la información pueden variar según la organización y su contexto, pero suelen incluir la protección de la información y los sistemas contra amenazas internas y externas, la prevención de interrupciones en los servicios y la minimización de los riesgos asociados con la gestión de la información.

2.2 Vulnerabilidades y amenazas

De acuerdo al autor [3] son conceptos muy importantes en la seguridad de la información, se consideran amenazas a toda acción o evento que tiene potencial de causar daño y puede llegar a comprometer los pilares de la seguridad informática los cuales son confidencialidad, integridad o disponibilidad de la información, además puede comprometer la operación de una organización. Estas amenazas pueden tener origen de varias fuentes y formas, como desastres naturales, errores humanos hasta ataques de “malware”.

Amenazas externas

El autor [5] menciona que estas provienen de fuentes fuera de una organización

o sistema, pueden incluir ataques de hackers, malware, phishing y otros tipos de ataques cibernéticos que buscan explotar vulnerabilidades en los sistemas de una organización. Las amenazas externas pueden ser especialmente peligrosas porque a menudo son difíciles de detectar y pueden ser muy sofisticadas. Las organizaciones deben tomar medidas para protegerse contra las amenazas externas, como implementar medidas de seguridad robustas y mantenerse actualizadas sobre las últimas tendencias y técnicas de ataque.

Existen varios tipos de amenazas cibernéticas que podemos detallar a continuación:

“Malware”: software malicioso diseñado para alterar, dañar o robar información de un sistema o red.

Ataques de denegación de servicio (DDoS): buscan abrumar un sistema o red con tráfico o solicitudes falsas para provocar que el sistema sea inaccesible.

Phishing: ataque de ingeniería social que utiliza información falsa para engañar a los usuarios de tal manera que revelen información confidencial, como contraseñas o información de tarjetas de crédito.

Ataques de fuerza bruta: con este procedimiento se intenta adivinar contraseñas o claves de cifrado mediante la prueba de múltiples combinaciones hasta encontrar la correcta.

“Ransomware”: es un tipo de “malware” que cifra los datos de un sistema y exige un pago para desbloquearlos.

Ataque de inyección de código: son ataques que aprovechan las

vulnerabilidades en el software para insertar código malicioso en un sistema o red.

Ataque de hombre en el medio: El objetivo de este ataque es interceptar la comunicación entre un emisor y un receptor para robar información o modificar datos.

Suplantación de identidad: Se utiliza información falsa para hacerse pasar otra persona o entidad con el fin de obtener acceso no autorizado a un sistema o red.

Amenazas internas

Menciona el autor [5] que provienen de fuentes dentro de una organización o sistema. Estas amenazas pueden incluir acciones maliciosas de empleados, contratistas o socios comerciales, así como errores no intencionales, como la pérdida de dispositivos o la divulgación accidental de información confidencial. Las amenazas internas pueden ser especialmente peligrosas porque los atacantes ya tienen acceso a los sistemas y datos de la organización, lo que puede hacer que sea más fácil para ellos llevar a cabo un ataque exitoso. Las organizaciones deben tomar medidas para protegerse contra las amenazas internas, como implementar políticas de seguridad sólidas, limitar el acceso a los datos y sistemas críticos y monitorear de cerca las actividades de los empleados y otros usuarios autorizados.

Entre las amenazas internas principalmente podemos mencionar las siguientes:

Amenazas involuntarias: causadas por errores no intencionales cometidos

por empleados o usuarios autorizados. Por ejemplo, la pérdida de un dispositivo que contiene información confidencial o la divulgación accidental de información a través de un correo electrónico.

Amenazas intencionales: causadas por empleados o usuarios autorizados que actúan de manera malintencionada. Por ejemplo, un empleado que roba información confidencial o un usuario que instala “malware” en un sistema.

Amenazas de terceros: causadas por contratistas, proveedores o socios comerciales que tienen acceso a los sistemas o datos de una organización. Por ejemplo, un contratista que instala un software malicioso en un sistema o un proveedor que divulga información confidencial a un competidor.

Amenazas naturales

Las amenazas naturales en el contexto de la seguridad informática hacen referencia a condiciones o eventos originadas por la naturaleza y podrían tener un impacto en los sistemas de información y la infraestructura tecnológica.

Entre las amenazas naturales más probables podemos identificar terremotos, inundaciones, tormentas, clima extremo, erupciones volcánicas.

Vulnerabilidades

Por su parte una vulnerabilidad hace referencia a un punto débil o fallo en una infraestructura o sistema informático que puede ser explotado y comprometer la seguridad, podemos clasificar las vulnerabilidades en:

Vulnerabilidades de configuración: ajustes de sistemas o aplicaciones que

no cumplen con las buenas prácticas en función de la seguridad.

Vulnerabilidades de hardware: hacen referencia a errores de fabrica o diseño de dispositivos.

Vulnerabilidades de software: Limitaciones en la programación de las aplicaciones que podrían ser explotadas.

Es importante identificar y mitigar tanto las vulnerabilidades como las amenazas para garantizar la seguridad de la información y los sistemas de información. Las vulnerabilidades pueden ser mitigadas mediante la aplicación de parches de seguridad, configuraciones adecuadas, actualizaciones de software, entre otras medidas. Las amenazas pueden ser mitigadas mediante la implementación de medidas de seguridad adecuadas, como “firewalls”, sistemas de detección de intrusiones, políticas de seguridad, entre otros, mencionado por el autor [3].

2.3 Hacking Ético

El autor [2] menciona al Ethical hacking como un conjunto de técnicas y herramientas utilizadas para evaluar la seguridad de los sistemas informáticos y redes, con el objetivo de identificar vulnerabilidades y debilidades que podrían ser explotadas por atacantes malintencionados, es una práctica cada vez más importante debido a la creciente dependencia de los sistemas informáticos y la necesidad de proteger la información sensible de las organizaciones.

Por parte del autor [6] se menciona que el Ethical hacking es un proceso donde intervienen profesionales de seguridad informática para intentar penetrar la

infraestructura tecnológica de una organización con el objetivo de encontrar vulnerabilidades para su tratamiento y mitigación, además menciona la importancia de tener las autorizaciones necesarias por parte de la organización antes de comenzar la evaluación de seguridad y se debe definir claramente el alcance y los objetivos de la evaluación.

Podemos mencionar que los principales objetivos del hacking ético son la identificación de vulnerabilidades, evaluar la postura de seguridad de una organización, reducir el riesgo de sufrir un ataque informático mejorando la seguridad a base de soluciones y recomendaciones.

Para comprender mejor podemos citar lo indicado por el autor [7] quien indica que existen 5 fases al aplicar Ethical hacking:

Reconocimiento: recopilar información sobre el sistema o red objetivo.

Escaneo: uso de varias herramientas y técnicas para identificar puertos abiertos, servicios y vulnerabilidades en el sistema o red objetivo.

Obtención de acceso: implica explotar vulnerabilidades para obtener acceso no autorizado al sistema o la red objetivo.

Mantenimiento de acceso: establecer una presencia persistente en el sistema o red para recopilar toda la información posible.

Cubrimiento de huellas: Eliminar cualquier evidencia del ataque y restaurar el sistema o la red a su estado original.

2.4 Técnicas de Penetración

El autor [8] menciona que las pruebas de penetración son la piedra angular de la defensa activa contra los ataques de seguridad cibernética. Conocer la vulnerabilidad y los puntos de exposición de una red o sistema es uno de los primeros pasos en una defensa activa del sistema.

Otro autor [9] enfoca a un pen test como un ataque intencional a un sistema informático o red, realizado con el objetivo de buscar debilidades en su seguridad, logrando así acceder a las características y datos del sistema informático, siendo una actividad preventiva que permite determinar si la información es segura.

La importancia de las pruebas de penetración mencionadas por el autor [10] radica en que permiten evaluar la seguridad de la infraestructura de TI de una organización al exponer de manera segura las vulnerabilidades existentes. Esto ayuda a identificar los riesgos y a gestionarlos para lograr estándares de seguridad más altos. Además, las pruebas de penetración ayudan a evaluar la eficacia de las herramientas y políticas de defensa en su lugar y a identificar las áreas que necesitan mejoras. Al realizar pruebas de penetración de manera regular, las organizaciones pueden reducir las pérdidas financieras y de información que podrían haber causado la pérdida de confianza de los clientes debido a violaciones de seguridad. También ayuda a las organizaciones a cumplir con los requisitos de los reguladores de la industria, los clientes y los accionistas, lo que ayuda a desarrollar la confianza, la imagen corporativa y a racionalizar las inversiones en seguridad de TI. En resumen, las pruebas de

penetración son una herramienta importante para garantizar la seguridad de la infraestructura de TI y proteger los activos de la organización.

Metodologías de pruebas de penetración

Menciona el autor [11] algunas metodologías de pruebas de penetración que han sido revisadas en varios estudios, entre ellos:

OSSTMM (Open-Source Security Testing Methodology Manual)

Es uno de los estándares de pruebas de penetración más utilizados y reconocidos. Se basa en un enfoque científico de las pruebas de penetración que contiene guías adaptables para los evaluadores. Puede utilizar esto para realizar una evaluación precisa.

OWAST (Open Web Application Security Project)

Corresponde a guías de pruebas para servicios web, en la nube, aplicaciones móviles (Android/IOS) y firmware.

Penetration testing execution standard (PTES)

Define las pruebas de penetración en 7 fases, las directrices de PTES brindan sugerencias practicas sobre procedimientos de pruebas y recomendaciones para herramientas de pruebas de seguridad.

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling

- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

NIST (National Institute of standards and Technology)

Ofrece una metodología de pentesting muy específica para pentesters para ayudarles a mejorar la precisión de la prueba. Tanto las empresas grandes como las pequeñas, de diversas industrias.

PTES (Penetration Testing Execution Standard)

Es una metodología pentest diseñada por un equipo de profesionales de seguridad de la información. El objetivo de PTES es crear un estándar completo y actualizado para las pruebas de penetración, así como crear conciencia entre las empresas sobre qué esperar de un pentest.

ISSAF (Information System Security Assessment Framework)

Es una guía de pentesting respaldada por Open Information Systems Security Group. Esta es una de las metodologías de prueba de seguridad que ya no se actualiza, por lo que está un poco sin datos. Sin embargo, todavía se utiliza por su naturaleza integral: vincula diferentes pasos del proceso de pentest con

herramientas relevantes.

Herramientas de penetración

Podemos citar al autor [10] donde se mencionan las siguientes herramientas:

Nmap: Es una herramienta de escaneo de puertos y detección de sistemas operativos.

Metasploit: Es un marco de pruebas de penetración que permite la ejecución de exploits y la realización de pruebas de vulnerabilidad.

Wireshark: Es un analizador de protocolos de red que permite la captura y análisis de tráfico de red.

Nessus: Es un escáner de vulnerabilidades que permite la identificación de vulnerabilidades en sistemas y aplicaciones.

Burp Suite: Es una herramienta de pruebas de penetración para aplicaciones web que permite la identificación de vulnerabilidades en aplicaciones web.

John the Ripper: Herramienta de cracking de contraseñas que permite la identificación de contraseñas débiles.

Hydra: Herramienta de cracking de contraseñas que permite la identificación de contraseñas débiles en servicios de red.

Continuando con esta revisión menciona el autor [9] lo siguiente, las herramientas disponibles para realizar Penetration Testing tienen diferentes grados de complejidad, y el manejo de algunas de ellas puede suponer un

desafío para la inteligencia y sagacidad del atacante, también conocido como pen-tester. Entre estas herramientas, se pueden mencionar escáneres de puertos, algoritmos complejos para descifrar contraseñas, sistemas de intrusión de fuerza bruta, herramientas de rastreo de redes y penetración de firewalls, así como herramientas de escaneo de vulnerabilidades de aplicaciones web y otras.

2.5 Gestión de incidentes

Un incidente se refiere a un evento no deseado o inesperado que afecta a los activos de información de una organización y que puede causar daño o pérdida de información.

Las fases de la gestión de incidentes indicadas por el autor [12] son las siguientes:

La primera fase es la detección del incidente, que puede ser realizada por el personal de seguridad, el personal de TI o los usuarios finales. La detección puede ser automática o manual, y puede ser el resultado de una alerta generada por un sistema de monitoreo o una notificación de un usuario.

Una vez que se ha detectado un incidente, se debe registrar en un sistema de gestión de incidentes. Esto incluye información sobre el incidente, como la fecha y hora de detección, la descripción del incidente y la prioridad.

La evaluación del incidente es la siguiente fase, en la que se determina la gravedad del incidente y se establece un plan de acción. La evaluación puede

ser realizada por el personal de seguridad, el personal de TI o un equipo de respuesta a incidentes.

La fase de contención es la siguiente, en la que se toman medidas para contener el incidente y evitar que se propague. Esto puede incluir la desconexión de sistemas afectados, la eliminación de “malware” o la restauración de copias de seguridad.

La fase de investigación es la siguiente, en la que se lleva a cabo una investigación para determinar la causa raíz del incidente y cómo se puede prevenir en el futuro. La investigación puede ser realizada por el personal de seguridad, el personal de TI o un equipo de respuesta a incidentes.

La fase de resolución es la siguiente, en la que se implementan medidas para resolver el incidente y restaurar los sistemas afectados a su estado normal. Esto puede incluir la instalación de parches de seguridad, la eliminación de “malware” o la restauración de copias de seguridad.

Finalmente, la fase de cierre implica la documentación del incidente y la realización de una revisión post-incidente para identificar lecciones aprendidas y oportunidades de mejora. La revisión post-incidente puede ser realizada por el personal de seguridad, el personal de TI o un equipo de respuesta a incidentes.

CAPITULO III

LEVANTAMIENTO DE INFORMACIÓN DE LA RED DE DATOS

3.1 Inventario de hardware y software

El inventario de hardware y software en una red de datos es esencial para la gestión eficiente y segura de recursos tecnológicos. Proporciona una visión precisa de los activos, facilitando la identificación y corrección de vulnerabilidades, previniendo pérdidas de datos y contribuyendo a la planificación y escalabilidad. Además, permite el mantenimiento proactivo, cumple con requisitos normativos, apoya el soporte técnico, contribuye a la continuidad del negocio, optimiza costos y respalda la toma de decisiones informada sobre inversiones en tecnología y mejoras de seguridad. En

resumen, el inventario fortalece la seguridad, eficiencia y planificación estratégica de una organización.

Para obtener la información de los activos fue necesario planificar reuniones con la gerencia de TI de la empresa, como parte de esta revisión en conjunto con personal de la empresa podemos definir las siguientes categorías para el inventario realizado:

Activos de hardware: Componentes físicos del sistema informático de la organización.

Activos de software: Programas y aplicaciones informáticas que forman parte integral de la infraestructura tecnológica de la organización.

Servicios: Funciones, aplicaciones o recursos que son implementados por sistemas informáticos.

Tabla 1: Inventario de activos

Código activo	Tipo activo	Descripción	Responsable
HW01	HW	Servidor desarrollo 1	Ing. TI
HW02	HW	Servidor desarrollo 2	Ing. TI
HW03	HW	Servidor desarrollo 3	Ing. TI
HW04	HW	Switch 24 puertos	Ing. TI
HW05	HW	Patch panel	Ing. TI
HW06	HW	Router VPN	Ing. TI
HW07	HW	Router Internet	Ing. TI

S01	S	SVN (Sistema control versiones)	Ing. TI
S02	S	Team City (Sistema generador de versiones) HW03	Ing. TI
S03	S	Microsoft SQL Server (BD) HW2, HW3	Ing. TI
SW01	SW	Visual Studio	Ing. TI
SW02	SW	Microsoft SQL Server Management	Ing. TI
SW03	SW	Notepad ++	Ing. TI
S04	S	Servicio Escritorio remoto	Ing. TI

Fuente: Elaboración propia

3.2 Topología de la red

La topología de red en una empresa tiene un impacto significativo en el rendimiento y eficiencia operacional. Es crucial analizar en detalle aspectos como la disposición de los nodos, las conexiones entre ellos, y la eficiencia energética. Al referirse a la eficiencia energética, resulta relevante no solo la eficiencia operativa sino también el consumo de energía, ya que esto puede afectar tanto los costos como el impacto medioambiental de la empresa.

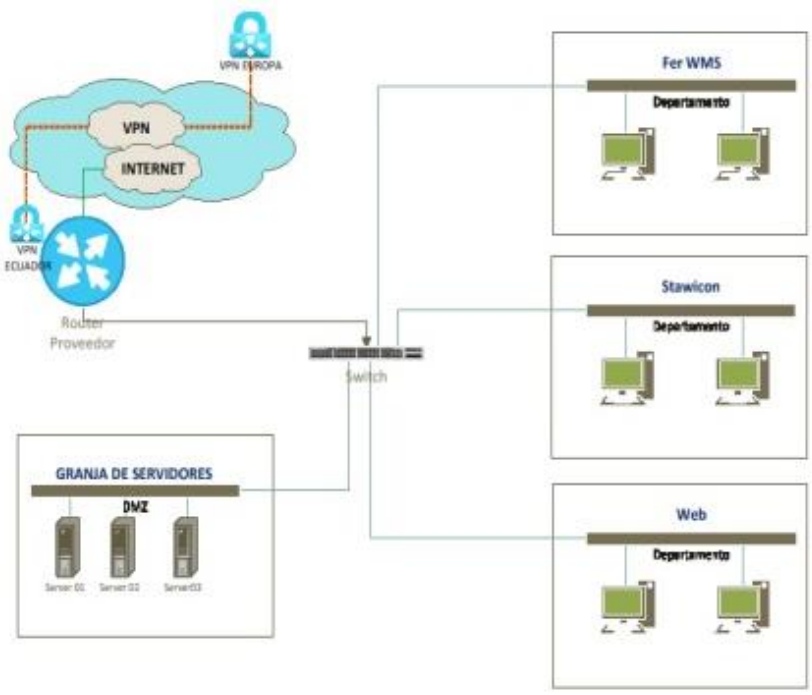

Figura 3.1. Topología de la red

Fuente: Elaboración propia

Identificación de sistemas operativos y licenciamiento

Identificar los sistemas operativos permite gestionar eficientemente las actualizaciones y parches de seguridad lo cual es de gran importancia para mitigar vulnerabilidades y reducir riesgos de ataques informáticos.

Además, contar con un inventario preciso de licencias ayuda a cumplir con requisitos legales y estar preparados para una futura auditoria de software por otra parte es de vital importancia para la planificación de la continuidad de las operaciones ya que permite anticipar y abordar problemas potenciales que podrían comprometer datos sensibles.

Tabla 2: Inventario de licencias

#Licencia	Nombre del software	Proveedor	Descripción
001	Windows Server 2008 R2	Microsoft	Versión Estándar instalado en HW01
002	Windows Server 2019	Microsoft	Versión estándar instalado en HW03
003	Windows Server 2016	Microsoft	Versión estándar instalado en HW02
004	Visual Studio 2013	Microsoft	Versión estándar
005	Visual Studio 2019	Microsoft	Versión estándar
006	Visual Studio 2022	Microsoft	Versión estándar
007	SQL Server 2019	Microsoft	Versión developer
008	SQL Server 2022	Microsoft	Versión developer
009	Team City	Jetbrains	Versión gratuita
010	Escritorio remoto VS	Microsoft	Versión estándar

Fuente: Elaboración propia

3.3 Levantamiento de controles de acceso

Existen usuarios de directorio activo en Alemania para el acceso a los servidores locales en Ecuador.

Cada servidor tiene un super usuario para configuraciones locales cuando sea necesario acceder desde la red local ya que la administración es compartida con personal de TI en Alemania.

Los accesos tanto físicos como a nivel de software están definidos únicamente para el equipo de TI en Ecuador para 3 personas.

Existen usuarios que mantienen cuentas de administrador en el directorio activo

además de las cuentas de usuarios estándar.

El acceso a las BD dentro de los servidores es a nivel general ya que se manejan datos de preproducción donde no se compromete información sensible para la empresa.

3.4 Revisión física de los activos de información

El proceso de revisión de los activos de información de la empresa de desarrollo de software realizado durante los primeros días del mes de diciembre 2023, donde se pudo evaluar la integridad y seguridad de los activos tecnológicos críticos para la operación de la empresa.

Para este proceso se llevó a cabo un plan detallado que incluye la identificación de activos, localización física, verificación de conexiones, validar estado físico de los equipos y las medidas de seguridad física implementadas en la gestión de estos activos.

Los resultados obtenidos durante esta revisión podemos mencionar que se documentaron los activos claves para nuestro estudio de seguridad como servidores, router, rack, ups, generadores, cableado, switch. Además, se evaluó el estado físico de los equipos los cuales mantienen al momento de nuestra revisión un estado general satisfactorio para la operación, se observó que los servidores se encuentran en una sala asignada para la infraestructura de conectividad debidamente ubicados en un rack, cuentan con equipos UPS como un sistema de respaldo en caso de cortes de energía adicional como contingencia mantienen un generador de energía eléctrica que abastece a todo el edificio donde se encuentran ubicadas las oficinas de la empresa.

En la revisión del cableado se verifico la integridad de las conexiones y la organización de los cables aquí se encontraron algunas novedades tales como el cruce de cables por el tumbado el cual no cuenta con la debida canalización y protección siendo vulnerable en caso de plagas o trabajos en dicha área, así mismo pudimos identificar que mantienen un etiquetado de manera correcta y el cableado se encontraba en buen estado.

Esta revisión física fue muy importante para identificar la integridad y seguridad de la infraestructura tecnológica. Además, este informe sirve como base para mejoras posteriores y tener una visión adecuada del estado de los activos de información físicos.

CAPITULO IV

DETERMINACION DE LAS AMENAZAS Y VULNERABILIDADES

4.1 Aplicación de técnicas de hacking y pruebas de penetración

Los Ethical Hacker son expertos que realizan una serie de medidas para determinar vulnerabilidades en sistemas informáticos con el fin de clasificar estas vulnerabilidades en base a sus niveles de riesgos además definir si estas vulnerabilidades se pueden explotar de forma segura y de manera controlada sin ocasionar daño a los sistemas que se están auditando para luego de eso elaborar un informe que se entregara a la organización con las recomendaciones necesarias de remediación.

Además, es importante mencionar que un Pentester es un Hacker Ético pero un Hacker Ético no necesariamente es un Pentester, al iniciar con la aplicación de

las técnicas de hacking se utilizará la metodología CEH (Certified Ethical Hacker) la cual consta de las siguientes fases.

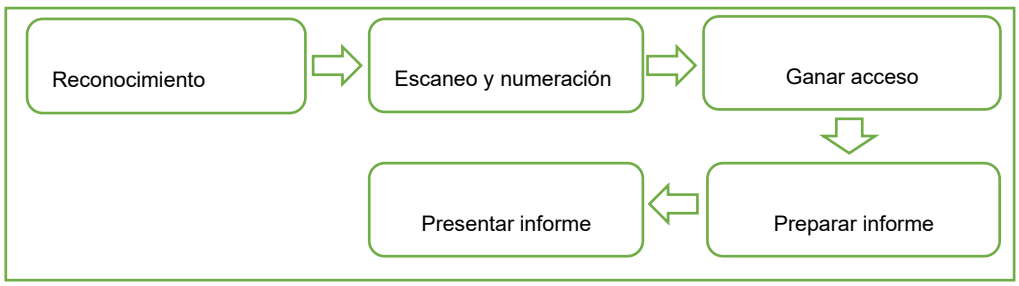

Figura 4.1. Fases técnicas de hacking

Fuente: Elaboración propia

Reconocimiento es el primer paso antes de planificar o analizar una posible intrusión a un sistema o red, también conocido como huella identificativa o footprinting. En esta etapa los objetivos son obtener toda la información que se encuentre disponible como nombre de dominio, direcciones ips, servidores de correo.

Para identificar el nombre del dominio utilizamos el navegador Tor el cual protege la identidad del remitente a través del envió de datos mediante nodos cifrados.

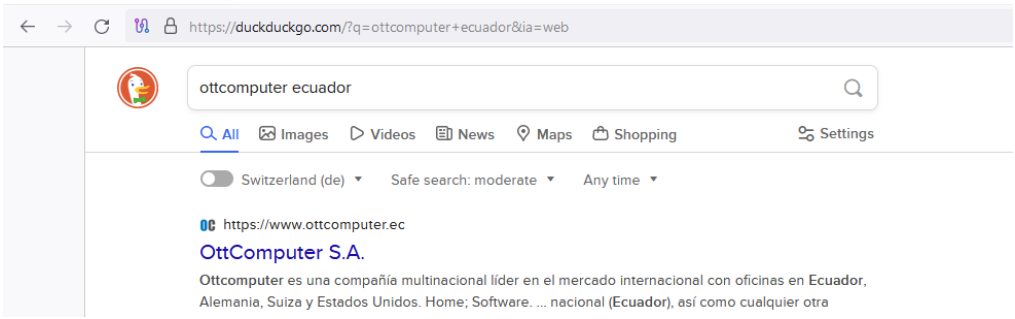

Figura 4.2. Búsqueda de dominio de la empresa

Fuente: Buscador de internet duckducgo.com

Se utiliza la consulta de dominio local para obtener más información disponible de manera pública.

Figura 1.3. Consulta del dominio en nic.ec

Fuente: nic.ec

4.2. Escaneo de red y exploración de puertos y servicios

En esta etapa se realiza una exploración de puertos y servicios con el fin de evaluar la postura y nivel de seguridad de la empresa, para la obtención de la dirección ip del dominio se utiliza la herramienta nslookup.

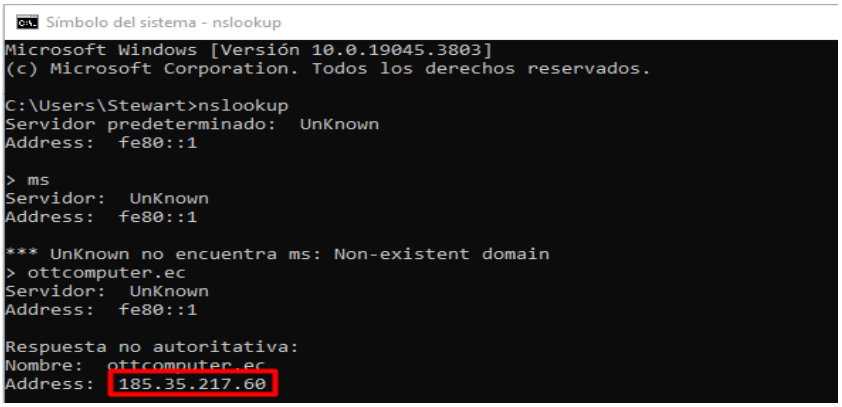

Figura 4.4. Obtención de la ip de dominio con nslookup

Fuente: Elaboración Propia

Además, podemos realizar este procedimiento mediante un ping al sitio web, donde podemos analizar la respuesta de la dirección ip del host y confirmamos que el sitio no se encuentra en un hosting ya que nos responde la misma ip identificada para el dominio.

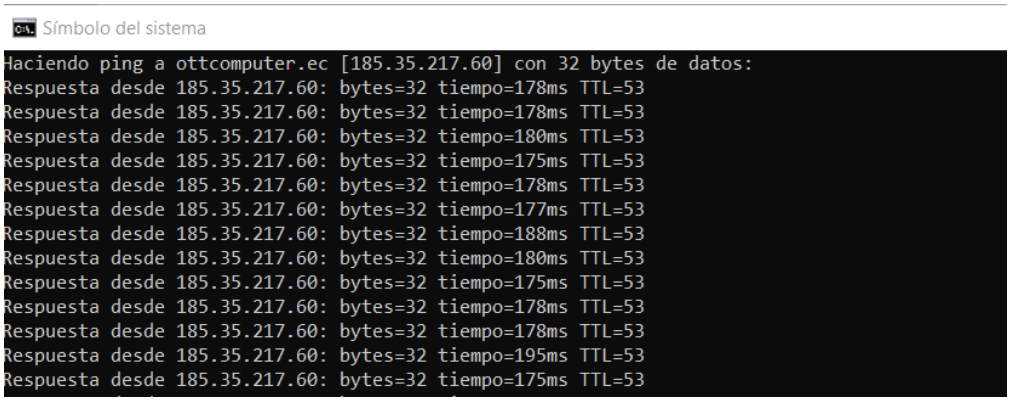

Figura 4.5. Ping al nombre de dominio

Fuente: Elaboración propia

Con el uso de la herramienta Maltego en una maquina con SO Kali Linux se realiza el proceso de footprinting a partir del nombre de dominio tal como podemos observar en el anexo C.

En este paso se realiza un reconocimiento con la herramienta nmap para identificar puertos y servicios.

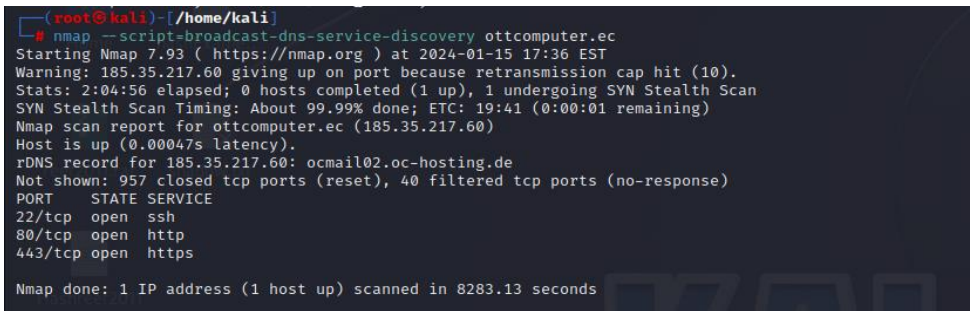

Figura 4.6. Resultado de ejecutar un script de

Fuente: Elaboración propia

Se utiliza la herramienta “dnsenum” la cual permite capturar toda la información que sea posible sobre el dominio.

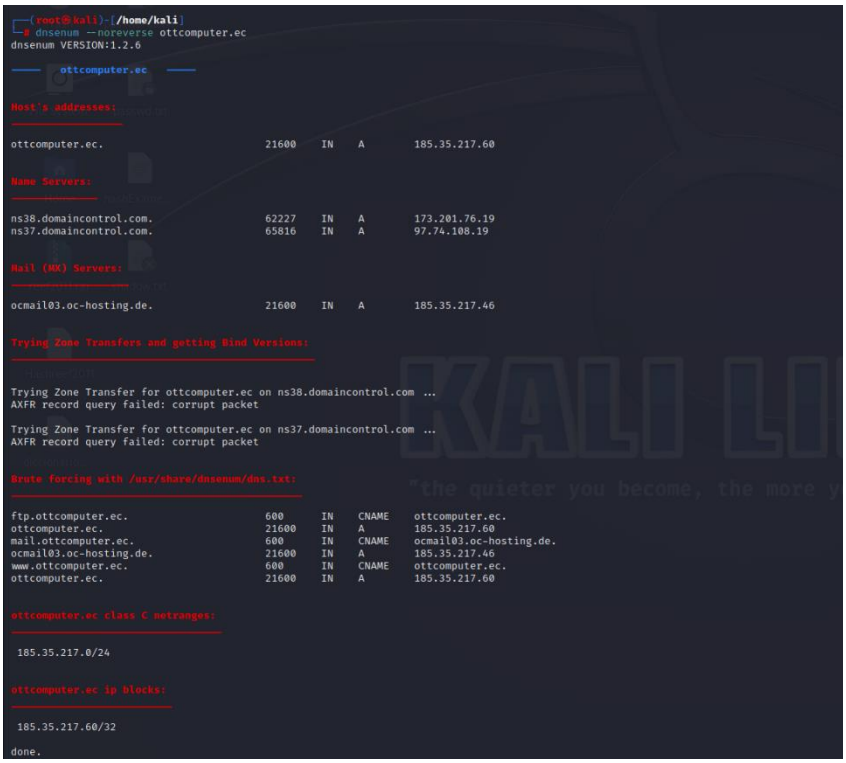

Figura 4.7. Identificación con herramienta dnsenum

Fuente: Elaboración propia

4.3. Análisis de vulnerabilidades lógicas y físicas

Vulnerabilidades físicas: Como parte del análisis realizado a la empresa de desarrollo de software en su estructura física se pueden identificar varios las siguientes vulnerabilidades:

Control de acceso: se maneja únicamente con una garita general que verifica el ingreso de personas en todo el edificio con un protocolo general, en las oficinas donde funciona la empresa no existe un protocolo que limite el acceso únicamente a personal autorizado.

Continuando con la revisión física se identifica que no existe un sistema de

cámaras de seguridad tanto en el punto de ingreso como tampoco dentro de las instalaciones.

Inventario de equipos: de acuerdo con la información proporcionada por el área de TI, al tratarse de una mediana empresa en el medio no cuentan con un inventario actualizado de sus activos físicos tampoco cuenta con un seguro sobre los equipos donde administran información sensible para la operación.

Respaldo de los datos: No cuenta con un plan de contingencia para el manejo de los datos que se almacenan en los servidores de desarrollo y datos sensibles para la operación, actualmente este proceso se lo realiza a nivel local cargando la data en discos externos.

Prevención de incendios: Las instalaciones de la empresa cuentan con un sistema de prevención de incendios debidamente instalado con activación mediante sensores además mantiene estratégicamente ubicados extintores en buen estado disponibles para una emergencia.

Ubicación del cableado: Durante la inspección se identifica que el cableado se encuentra sobre el tumbado y llega a cada punto de red entre las paredes de yeso, aunque el cableado se encuentra en buen estado este no cuenta con una debida canalización que lo proteja de amenazas y atenuación tomando en consideración que sobre el tumbado también pasa cableado eléctrico.

Armario de conexión: El armario donde se encuentran ubicados los servidores es un espacio físico cerrado sin embargo este lugar no cuenta con un control de acceso para personal autorizado únicamente.

Etiquetado de cables: Durante la evaluación no se encuentra documentación que permita tener el soporte de la correlación de etiquetas con la ubicación y función de los puertos de red habilitados.

Pruebas periódicas de integridad: Durante la evaluación se verifica que no existe un plan de pruebas para validar la integridad del cableado y además identificar posibles problemas físicos o de seguridad.

Vulnerabilidades lógicas: En el escaneo se validan los siguientes puertos:

Tabla 3: Puertos y servicios identificados en el escaneo

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.9p1 10+deb10u2 (protocol 2.0)
80	http	Apache httpd 2.4.38
443	https	Apache httpd 2.4.38

Fuente: Christian Pulley

Utilizamos la herramienta nmap para identificar los puertos abiertos y servicios.

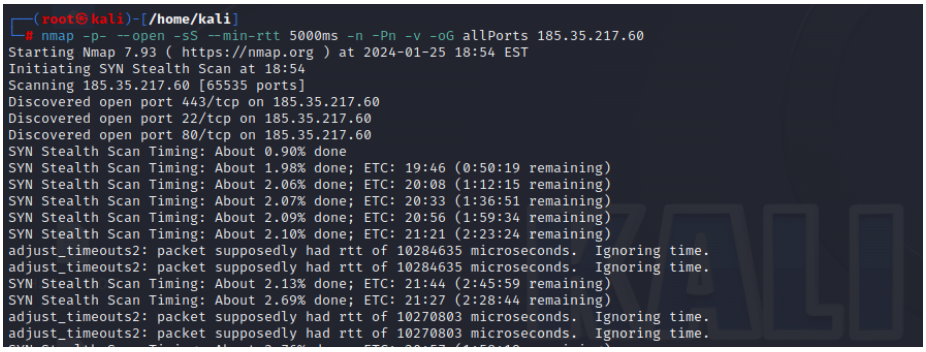

Figura 4.8. Escaneo con nnmap para identificar los puertos abiertos

Fuente: Elaboración propia

Podemos identificar que los puertos que se identifican abiertos pueden exponer a una serie de vulnerabilidades y riesgos de seguridad por ejemplo para el puerto 22 que es utilizado para el servicio SSH (secure shell) es vulnerable a distintos ataques, detallados a **continuación.**

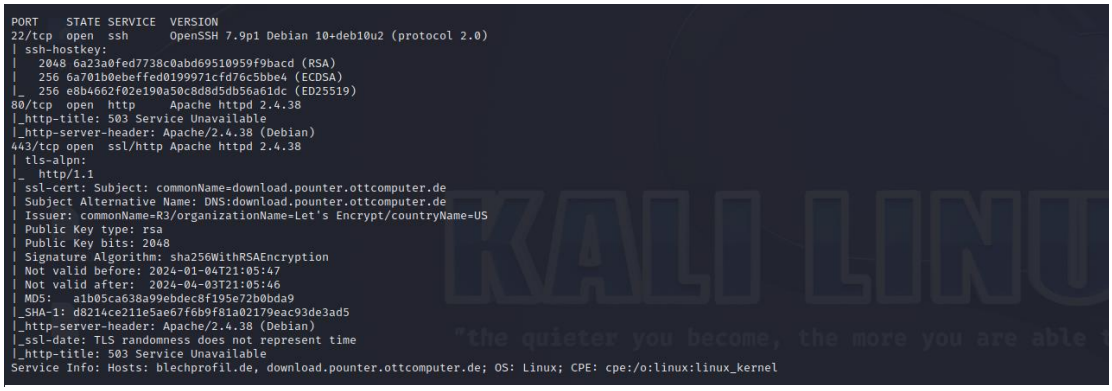

Figura 4.9. Escaneo con nmap detallado

Fuente: Elaboración propia

Software vulnerable: Si existe una versión obsoleta de software SSH esta podría ser explotada.

Ataques de fuerza bruta: la organización podría ser víctima de ataques de este tipo para intentar obtener información de credenciales.

Ataques MTM (Man-in-the-Middle): Existe el riesgo de una posible intersección de datos en la comunicación entre cliente y servidor.

Accesos no autorizados: Mediante el servicio SSH podría intentarse un acceso malicioso, en caso de no tener configuradas políticas de acceso.

Figura 2. Acceso vía SSH

Fuente: Elaboración propia

Al realizar una auditoria con la herramienta SSH-audit se obtienen los siguientes resultados, tal como muestra la imagen 12.

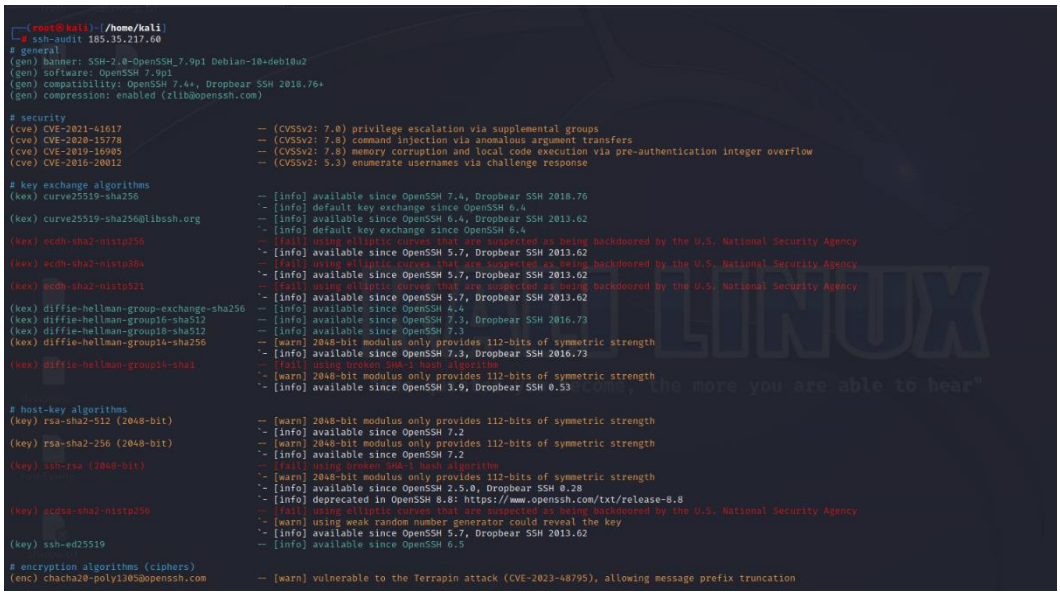

Figura 4.11. Uso herramienta ssh-audit para obtener información

Fuente: Elaboración propia

En la fase para ganar acceso se utiliza la herramienta enum4linux la cual nos permite obtener información de los usuarios que permiten acceder al servidor.

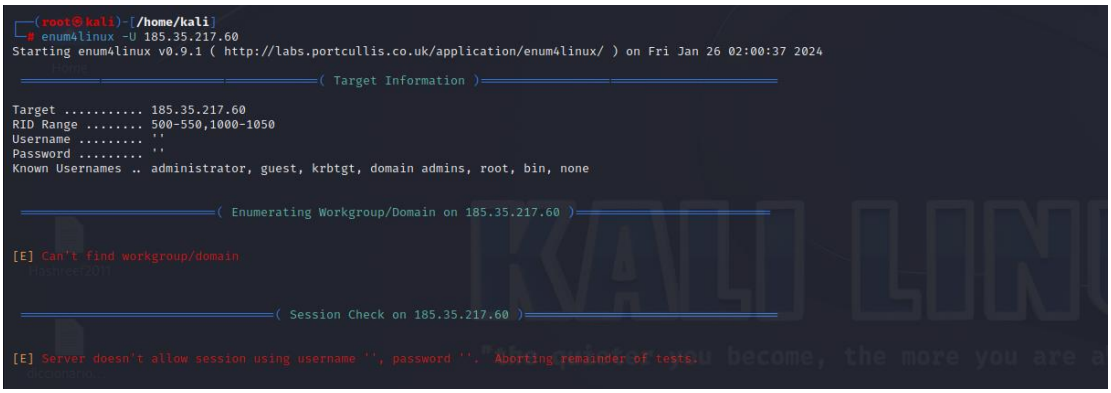

Figura 4.12. Uso herramienta enum

Fuente: Elaboración propia

Luego de obtener la lista de usuarios podemos tratar de obtener las contraseñas por un ataque de fuerza bruta, sin embargo, no realizaremos este paso por solicitud del área de TI de la empresa.

4.4. Análisis de riesgos

El análisis de riesgos en este estudio se realizó de manera cualitativa utilizando datos numéricos con el objetivo de cuantificar el impacto y probabilidad de los riesgos.

En este estudio se determinará el riego basado en el valor de los activos en función del grado de priorización para la organización, la evaluación del grado de protección que requiere cada activo depende del nivel de sensibilidad e importancia para la operación de la empresa. En este proceso se realiza una valoración a los activos de acuerdo con el grado de protección requerido.

Este proceso dará como resultado una métrica del potencial daño que podría afectar la operación de la organización en caso de la materialización de un riesgo. La escala de valoración definida la podemos visualizar en la siguiente tabla.

Tabla 4: Escala de valoración activos de información

Escala de valoración de los activos		
Escala	**Nomenclatura**	**Definición**
Muy alto	MA	Afectación muy alta
Alto	A	Afectación alta
Medio	M	Afectación media
Bajo	B	Afectación baja
Muy Bajo	MB	Afectación muy baja

Fuente: Elaboración propia

En la tabla 4 se ha asignado un nivel de valoración a los activos de información que forman parte de la topología en la empresa de desarrollo de software. El detalle de la evaluación de cada activo puede revisarse en el anexo A.

Tabla 5: Valoración de activos de información

ACTIVO	DESCRIPCIÓN	VALORACION
RO	Router propiedad del ISP	MUY ALTO
SD1	Servidor de desarrollo 1	MUY ALTO
SD2	Servidor de desarrollo 2	MUY ALTO
SD3	Servidor de desarrollo 3	MUY ALTO
SW1	Microsoft SQL server	ALTO
SW2	Microsoft SQL Server Management	ALTO

SW3	SVN (sistema control de versiones)	ALTO
SW4	Team City (Generador de versión)	ALTO
SW5	Servicio de escritorio remoto	ALTO
HW1	Switch interno	MEDIO
HW2	Router VPN	MEDIO
HW3	Router Wifi	MEDIO
HW4	Patch Panel	BAJO

Fuente: Elaboración propia

Evaluar la probabilidad e impacto sobre la materialización de amenazas es vital para gestionar los riegos a los cuales está expuesta toda organización, consideramos a la probabilidad como la medida de la posibilidad que ocurra un evento; por otra parte, la amenaza es la situación que podría presentarse en caso de darse una situación no deseada. En base a este análisis se podrá identificar el grado de magnitud de un riesgo

y la probabilidad asociada a su ocurrencia, lo cual permitirá identificar, priorizar y mitigar eficazmente los riegos dentro de la operación que posibiliten una gestión proactiva que aborde los riesgos identificados.

En la siguiente tabla nos detalla distintos criterios para considerar en la medición del riesgo sin embargo es importante tomar en cuenta el modelo de negocio de la organización, también factores internos y externos que pueden afectar la operación.

Tabla 6: Criterios para medir el riesgo

Impacto	¿Qué tan grave sería el impacto de un evento de riesgo?
-Financiero	-No financiero
-Ingresos	Reputación
-Costo de recuperación	-Legal
	Operaciones
Probabilidad	**¿Qué tan probable es que este evento de riesgo se produzca en un plazo determinado?**
¿Con qué frecuencia se han presentado eventos de riesgo en el pasado?	
Velocidad de materialización	**¿Qué tan rápido podría ocurrir este evento de riesgo?**
Tiempo que se tendría para reaccionar	
Efectividad en la administración del riesgo	**¿Qué tan efectivos son los procesos de gestión y técnicas de mitigación para hacer frente a los riegos?**
-Capacidad de prevención	
-Capacidad de detección	
-Capacidad de recuperación	
Vulnerabilidad	**¿Considerando los puntos anteriores cuál es la vulnerabilidad al riesgo por parte de la organización?**
-Nivel de exposición	
-Magnitud de incidencia a eventos de riesgo	
Impacto	**¿Qué tan grave sería el impacto de un evento de riesgo?**
-Financiero	-No financiero
-Ingresos	-Reputación
-Costo de recuperación	-Legal
	-Operaciones

Probabilidad	**¿Qué tan probable es que este evento de riesgo se produzca en un plazo determinado?**
¿Con qué frecuencia se han presentado eventos de riesgo en el pasado?	
Velocidad de materialización	**¿Qué tan rápido podría ocurrir este evento de riesgo?**
Tiempo que se tendría para reaccionar	
Efectividad en la administración del riesgo	**¿Qué tan efectivos son los procesos de gestión y técnicas de mitigación para hacer frente a los riegos?**
-Capacidad de prevención	
-Capacidad de detección	
-Capacidad de recuperación	
Vulnerabilidad	**¿Considerando los puntos anteriores cuál es la vulnerabilidad al riesgo por parte de la organización?**
-Nivel de exposición	
-Magnitud de incidencia a eventos de riesgo	

Fuente: Elaboración propia

Para la escala de probabilidad se ha definido un rango de 1 a 5, para lo cual 1 representa un evento de poca frecuencia y 5 un evento muy probable.

Tabla 7: Escala de probabilidad

Probabilidad	Descripción	Frecuencia
1	Inusual	Ocurrencia >= 10 años
2	Poco común	Ocurrencia 5–10 años
3	Posible	Ocurrencia 1-5 años

4	Probable	Ocurre varias veces al año
5	Casi seguro	Ocurre regularmente

Fuente: Elaboración propia

4.5 Mapa de calor

Es una herramienta muy efectiva para visualizar y analizar los riesgos, permitirá observar de manera intuitiva las áreas de mayor vulnerabilidad y las amenazas predominantes, lo cual facilitará la toma de decisiones para mitigar los riesgos.

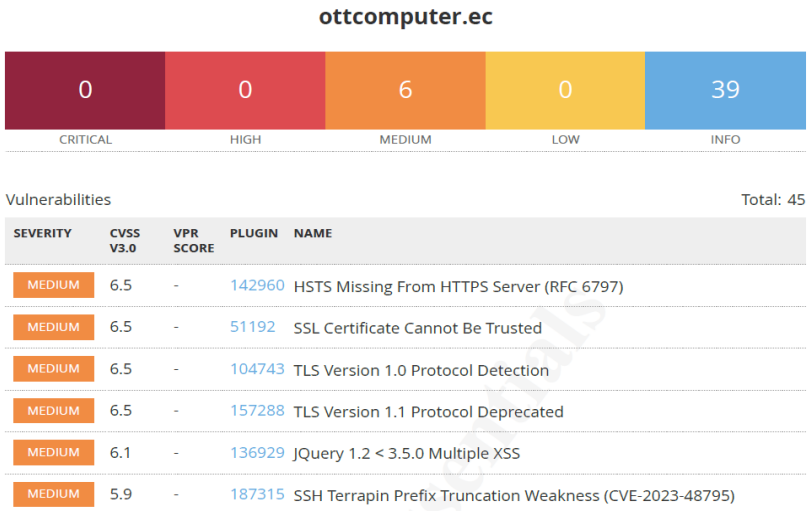

Figura 4.13. Analizando vulnerabilidades con la

Fuente: Nessus Essentials

Para realizar el mapa de calor se realiza un escaneo de vulnerabilidades con la herramienta Nessus donde se identifica lo siguiente en la clasificación media:

Basados en los resultados del análisis con Nessus se clasifican las vulnerabilidades en un mapa de calor de acuerdo con la siguiente escala de gravedad mostrada en la tabla 7.

Tabla 8: Escala de gravedad

	Riesgos	Impacto	Probabilidad
1	**Riesgo de pérdida de datos:** La empresa no cuenta con un plan de respaldo de la información lo cual con lleva el riesgo de pérdida de datos, afectación en los tiempos de recuperación, impacto en la productividad, perdida de reputación y confianza.	Alto	Alta
2	**Riesgo de control de acceso:** La empresa no cuenta con un protocolo para acceder a sus instalaciones lo que representa un riesgo al permitir acceso de personal no autorizado.	Alto	Medio
3	**Riesgo de hardening:** El servidor web remoto no utiliza HTTP Strict Transport Security, esto mantiene un riesgo de ataques MITM, exposición de credenciales como cookies de sesión.	Alto	Medio
4	**Riesgo de certificado SSL:** El certificado SSL presentado por el servicio web no es confiable, expone a riesgos de suplantación de identidad, exposición de datos sensibles, riesgos de seguridad en aplicaciones web.	Alto	Medio
5	**Riesgo de versión obsoleta de protocolo TLS:** Se encuentra en uso una versión obsoleta o menos segura del protocolo de capa de transporte el cual sirve para cifrar la comunicación entre cliente y el servidor lo cual expone a ataques de protocolo poodle, beast, falta de soporte y actualizaciones, incompatibilidad con estándares de seguridad.	Alto	Medio

Fuente: Elaboración propia

En el análisis de vulnerabilidades realizado, se ha utilizado una escala de gravedad para clasificar el impacto potencial de cada vulnerabilidad identificada. Esta escala de gravedad se define en tres niveles: Bajo, Medio y Alto. El nivel Bajo (1) indica que la vulnerabilidad tiene un impacto mínimo en la organización y sus operaciones. El nivel Medio (2) sugiere que la vulnerabilidad puede causar un impacto moderado, afectando ciertas áreas críticas, pero no comprometiendo la totalidad del sistema. Finalmente, el nivel Alto (3) representa vulnerabilidades con un impacto severo, las cuales pueden causar daños significativos a la integridad, disponibilidad y confidencialidad de los datos y servicios de la organización. Esta categorización es fundamental para priorizar las acciones de mitigación, enfocándose primero en aquellas vulnerabilidades clasificadas como de alto impacto y alta probabilidad de ocurrencia.

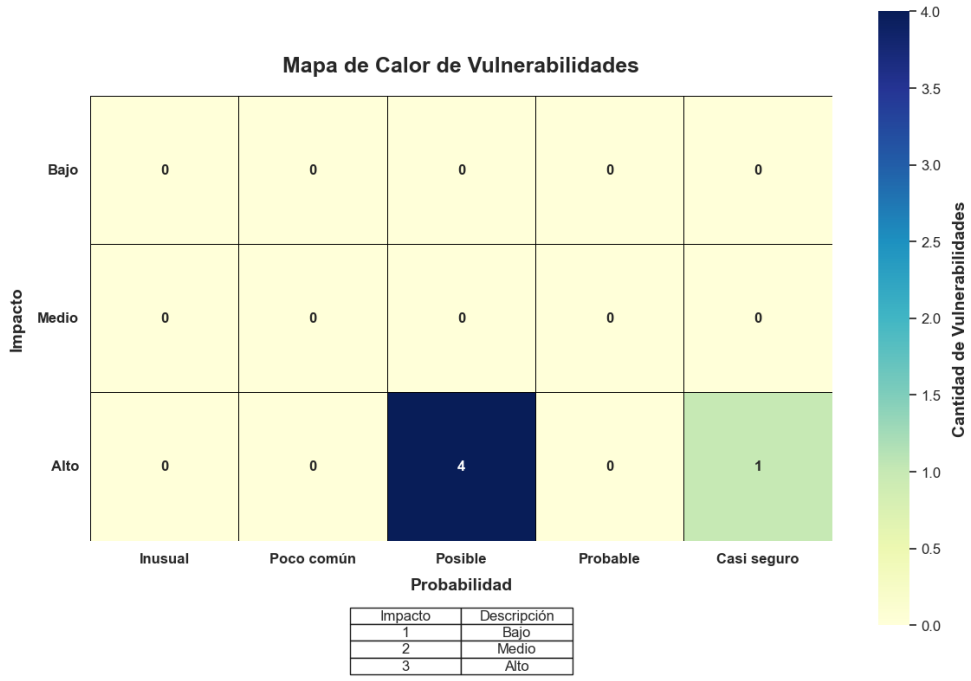

Figura 4.14. Mapa de vulnerabilidades

Fuente: Elaboración propia

En el mapa de calor tenemos una herramienta visual de gran valor para la evaluación y gestión de vulnerabilidades en la red de datos de la empresa de desarrollo de software. Este mapa presenta de manera clara y concisa las áreas de mayor riesgo, combinando la probabilidad de ocurrencia de los eventos con el impacto potencial de las vulnerabilidades. Las características principales del mapa de calor incluyen una codificación de colores que facilita la identificación rápida de las zonas críticas, anotaciones precisas que indican la cantidad de vulnerabilidades en cada categoría, y una tabla de referencia que define los niveles de impacto (Bajo, Medio y Alto). Los beneficios de utilizar este mapa de calor son múltiples: permite una priorización eficiente de las acciones correctivas, mejora la comunicación del estado de seguridad a los “stakeholders”, y proporciona una base sólida para la toma de decisiones estratégicas en materia de ciberseguridad. En conjunto, estas características y beneficios hacen del mapa de calor una herramienta indispensable para fortalecer la postura de seguridad de la organización.

CAPITULO V

DISEÑO DEL PLAN DE ACCIÓN PARA ABORDAR Y REMEDIAR LAS VULNERABILIDADES IDENTIFICADAS.

5.1 Asignar controles a los riegos

Como objetivo en este punto se desarrollará e implementará controles específicos para abordar los riesgos identificados en el análisis de vulnerabilidades, en línea con los estándares de la norma ISO/IEC 27001. Estos controles están destinados a mitigar los efectos potenciales de las vulnerabilidades y proteger los activos de la información de la empresa.

La metodología que se utilizará para asignar adecuadamente los controles a los riegos identificados se basa en la información que previamente se ha identificado de los riegos y vulnerabilidades.

Los controles se tomarán de la norma ISO 27001 anexo A, donde se detalla una lista de controles de seguridad en diferentes categorías, para lo cual se selecciona de acuerdo con cada riesgo identificado.

Cada riesgo se abordará asignando uno o más controles recomendados por la norma. Esta asignación se basará en la eficacia esperada del control para mitigar el riesgo y la viabilidad de su implementación.

Vulnerabilidad Identificada	Descripción	Control ISO/IEC 27001	Descripción del Control
Acceso no autorizado	Riesgo de acceso indebido a datos y sistemas críticos	A.9.1.1, A.9.1.2, A.9.4.2	Política de control de acceso, acceso a redes y restricción de información
Pérdida de datos por malware	Riesgo de infecciones por malware que pueden causar pérdida de datos	A.12.2.1	Implementación y actualización de software antivirus y antimalware
Falta de conciencia sobre seguridad	Riesgo de que empleados no estén al tanto de las políticas y prácticas de seguridad	A.7.2.2	Programas de formación y concienciación sobre la seguridad
Software desactualizado	Riesgo de explotación de vulnerabilidades en software no actualizado	A.12.6.1	Procesos para identificar y aplicar actualizaciones y parches de seguridad
Configuraciones de seguridad débiles	Riesgo de configuraciones incorrectas que pueden ser explotadas	A.14.2.1	Revisiones periódicas de las configuraciones de seguridad
Pérdida de datos por fallos de hardware	Riesgo de pérdida de datos por fallos en dispositivos físicos	A.12.3.1	Procedimientos de copias de seguridad para la protección de datos
Exposición a amenazas físicas	Riesgo de daños físicos a instalaciones y equipos	A.11.1.1, A.11.1.2	Controles físicos para proteger las instalaciones
Gestión inadecuada de incidentes	Riesgo de no detectar y responder adecuadamente a incidentes de seguridad	A.16.1.1, A.16.1.4	Procesos de gestión y respuesta a incidentes de seguridad
Uso no autorizado de dispositivos móviles	Riesgo asociado al acceso no controlado desde dispositivos móviles y entornos de teletrabajo	A.6.2.1, A.6.2.2	Políticas para el uso seguro de dispositivos móviles y prácticas de teletrabajo

Figura 10. 1. Controles ISO/IEC 27001 Aplicados a

Fuente: Norma ISO 27001

5.2 Selección de soluciones, contramedidas, tiempos y costos

En este análisis se detallará la selección de soluciones y contramedidas específicas para mitigar las vulnerabilidades identificadas en el análisis previo. Se evaluarán diferentes opciones considerando su efectividad, tiempo de implementación y costo. El objetivo es encontrar un balance óptimo entre

seguridad, tiempo y costos para asegurar la protección adecuada de los activos de información de la empresa de desarrollo de software.

La selección de soluciones y contramedidas, junto con la evaluación de tiempos y costos, es un paso crítico para la implementación efectiva de un plan de seguridad. Las soluciones propuestas deben equilibrar la efectividad en la mitigación de riesgos con la viabilidad financiera y temporal para la organización. Un enfoque estructurado y bien planificado permitirá a la empresa de desarrollo de software fortalecer significativamente su postura de seguridad y proteger sus activos de información contra amenazas y vulnerabilidades, este enfoque detallado asegura que cada vulnerabilidad sea tratada adecuadamente y que las soluciones implementadas sean sostenibles a largo plazo.

Vulnerabilidad Identificada	Solución / Contramedida	Tiempo de Implementación	Costo Estimado
Acceso no autorizado	Implementar políticas de control de acceso, sistemas de autenticación multifactor, y auditorías regulares de acceso	2 meses	$5,000
Pérdida de datos por malware	Desplegar software antivirus y antimalware, realizar actualizaciones periódicas	1 mes	$3,000
Falta de conciencia sobre seguridad	Implementar programas de formación y concienciación en seguridad para todos los empleados	3 meses	$2,500
Software desactualizado	Establecer un programa de gestión de parches y actualizaciones de software	1 mes	$2,000
Configuraciones de seguridad débiles	Realizar revisiones periódicas de configuraciones de seguridad y aplicar políticas de hardening	2 meses	$4,000
Pérdida de datos debido a fallos de hardware	Implementar y mantener procedimientos de copia de seguridad, establecer un sistema de recuperación ante desastres	3 meses	$7,000
Exposición a amenazas físicas	Implementar controles físicos de seguridad en las instalaciones, establecer procedimientos de acceso seguro	2 meses	$6,000
Gestión inadecuada de incidentes	Desarrollar e implementar un plan de respuesta a incidentes de seguridad, realizar simulacros periódicos	3 meses	$5,500
Uso no autorizado de dispositivos móviles	Desarrollar políticas de seguridad para dispositivos móviles, establecer controles de acceso seguro	1 mes	$3,500
Comunicaciones no seguras	Implementar políticas de cifrado para comunicaciones, utilizar VPNs para conexiones remotas	2 meses	$4,500

Figura 5.2. Soluciones y contramedidas

Fuente: Elaboración propia

5.3. Elaboración del plan

El Anexo B presenta un plan de acción detallado y estructurado para abordar y remediar las vulnerabilidades identificadas en la red de datos de la empresa. Este plan se divide en cinco fases principales: Asignar Controles a los Riesgos, Selección de Soluciones Contramedidas, Tiempos y Costos, Implementación de Controles y Validación, Capacitación y Concientización, y Monitoreo Continuo y Mejora Continua. Cada fase está claramente delineada con objetivos específicos y acciones concretas que describen los pasos a seguir. La columna de "Acciones" se ha formateado cuidadosamente para incluir listas con viñetas, proporcionando una presentación clara y fácil de seguir. Además, se han asignado responsables y herramientas específicas para cada acción, asegurando que las tareas sean ejecutadas de manera eficiente y eficaz. Este plan de acción, con sus detalladas instrucciones y asignaciones, proporciona una guía comprensiva para mejorar la seguridad de la red de datos y garantizar la protección continua de los activos de la empresa.

5.4. Beneficios de tener un plan

Implementar un plan de acción de seguridad detallado y estructurado ofrece numerosos beneficios para la empresa, especialmente en el ámbito de la protección de datos y la gestión de riesgos. A continuación, se describen los principales beneficios:

Mejora de la Postura de Seguridad

Un plan de acción de seguridad permite a la empresa identificar, evaluar y mitigar las vulnerabilidades en sus sistemas y redes de

manera sistemática. Esto mejora significativamente la postura de seguridad de la organización, reduciendo el riesgo de brechas de seguridad y ciberataques.

Cumplimiento Normativo

El plan de acción ayuda a la empresa a cumplir con las normativas y regulaciones de seguridad aplicables, como ISO/IEC 27001, GDPR, y otras leyes de protección de datos. El cumplimiento normativo no solo evita sanciones legales, sino que también mejora la reputación de la empresa ante clientes y socios.

Reducción de Costos

La identificación y mitigación proactiva de vulnerabilidades reduce los costos asociados a los incidentes de seguridad, como la pérdida de datos, interrupciones del servicio, y daños a la reputación. Además, un enfoque preventivo es generalmente más económico que reaccionar a incidentes después de que ocurran.

Mayor Eficiencia Operativa

Un plan de acción claro y estructurado proporciona una hoja de ruta para la implementación de medidas de seguridad, lo que facilita la coordinación entre diferentes departamentos y equipos. Esto mejora la eficiencia operativa y asegura que las medidas de seguridad se implementen de manera coherente y efectiva.

Protección de Activos Críticos

La clasificación y protección de activos críticos es una parte esencial del plan de acción. Esto asegura que los activos más importantes de la empresa, como datos sensibles y sistemas clave, reciban el nivel adecuado de protección, reduciendo el riesgo de pérdidas significativas.

Conciencia y Capacitación en Seguridad

El plan de acción incluye programas de capacitación y concientización en seguridad para todo el personal. Esto no solo mejora el conocimiento y la preparación de los empleados ante posibles amenazas, sino que también fomenta una cultura de seguridad dentro de la organización.

Respuesta Efectiva a Incidentes

Un plan de acción bien definido incluye procedimientos para la detección y respuesta a incidentes de seguridad. Esto asegura que la empresa pueda responder de manera rápida y efectiva a cualquier amenaza, minimizando el impacto de los incidentes y facilitando una recuperación rápida.

Mejora Continua

La implementación de un plan de acción de seguridad no es un proceso estático. El monitoreo continuo y la mejora del plan aseguran que la empresa se mantenga al día con las nuevas amenazas y

vulnerabilidades, adaptando sus medidas de seguridad en consecuencia.

CONCLUSIONES

En esta tesis, se ha desarrollado un enfoque integral para mejorar la seguridad informática de una empresa de desarrollo de software mediante la implementación de un plan de acción basado en técnicas de hacking ético y pruebas de penetración. A lo largo del proceso, se identificaron y evaluaron las vulnerabilidades presentes en la red de datos de la empresa, y se implementaron medidas correctivas para mitigar los riesgos asociados.

Los principales hallazgos de este estudio indican que una postura proactiva en la gestión de la seguridad informática, mediante la identificación temprana de vulnerabilidades y la aplicación de soluciones adecuadas, puede reducir significativamente el riesgo de incidentes de seguridad. Además, la implementación de un plan de acción estructurado y detallado no solo mejora la postura de seguridad de la empresa, sino que también facilita el cumplimiento normativo, reduce costos y aumenta la eficiencia operativa.

Se ha demostrado que la capacitación continua del personal y la promoción de una cultura de seguridad son elementos cruciales para mantener un entorno seguro. La respuesta rápida y eficaz a los incidentes de seguridad también es fundamental para minimizar el impacto de las amenazas y asegurar una recuperación rápida.

RECOMENDACIONES

Para asegurar la efectividad y sostenibilidad del plan de acción de seguridad, se recomienda realizar una revisión y actualización continua del plan cada seis meses. Esto permitirá a la empresa adaptarse a nuevas amenazas y vulnerabilidades de manera oportuna. Además, es fundamental implementar programas de capacitación en seguridad informática para todo el personal. Estos programas deben incluir talleres, seminarios y ejercicios prácticos que aborden las últimas amenazas y mejores prácticas de seguridad, fomentando una cultura de seguridad en toda la organización. El establecimiento de sistemas de monitoreo y auditoría continua también es crucial para detectar y responder a incidentes de seguridad en tiempo real, utilizando herramientas avanzadas como SIEM (Security Information and Event Management).

Asimismo, es vital mantener todas las herramientas y tecnologías de seguridad actualizadas con los últimos parches y versiones, y colaborar con expertos en seguridad informática y empresas especializadas para obtener una perspectiva externa objetiva. Promover una cultura de seguridad dentro de la organización es esencial, asegurando que todos los empleados comprendan la importancia de la seguridad informática y su responsabilidad en la protección de los activos de la empresa. Finalmente, desarrollar y aplicar políticas de seguridad claras y estrictas para el manejo seguro de la información y la respuesta a incidentes garantizará una defensa robusta contra ciberataques y contribuirá a la resiliencia general de la organización ante posibles amenazas.

BIBLIOGRAFÍA

[1] S. A. Saleem, «Ethical Hacking as a Risk Management Technique», en *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, en InfoSecCD ’06. New York, NY, USA: Association for Computing Machinery, 2006, pp. 201-203. doi: 10.1145/1231047.1231089.

[2] U. M. Khokhar y B. Tran, «Fundamentals of Ethical Hacking and Penetration Testing», en *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, en SIGITE ’19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 149-150. doi: 10.1145/3349266.3351391.

[3] Y. Jia-bin y G. Kai-kai, «Information Security Control in the Application of Grid Security», en *Proceedings of the 2007 Asian Technology Information Program’s (ATIP’s) 3rd Workshop on High Performance Computing in China: Solution Approaches to Impediments for High Performance Computing*, en CHINA HPC ’07. New York, NY, USA: Association for Computing Machinery, 2007, pp. 198-202. doi: 10.1145/1375783.1375822.

[4] S. Fenz y A. Ekelhart, «Formalizing Information Security Knowledge», en *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, en ASIACCS ’09. New York, NY, USA: Association for Computing Machinery, 2009, pp. 183-194. doi: 10.1145/1533057.1533084.

[5] H. Kettani y R. M. Cannistra, «On Cyber Threats to Smart Digital Environments», en *Proceedings of the 2nd International Conference on Smart Digital Environment*, en ICSDE’18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 183-188. doi: 10.1145/3289100.3289130.

[6] L. Epling, B. Hinkel, y Y. Hu, «Penetration Testing in a Box», en *Proceedings of the 2015 Information Security Curriculum Development Conference*, en InfoSec ’15. New York, NY, USA: Association for Computing Machinery, 2015. doi: 10.1145/2885990.2885996.

[7] A. Y. Ding, G. L. De Jesus, y M. Janssen, «Ethical Hacking for Boosting IoT Vulnerability Management: A First Look into Bug Bounty Programs and Responsible Disclosure», en *Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing*, en ICTRS ’19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 49-55. doi: 10.1145/3357767.3357774.

[8] A. Falah, L. Pan, y M. Abdelrazek, «Visual Representation of Penetration Testing Actions and Skills in a Technical Tree Model», en *Proceedings of the Australasian Computer Science Week Multiconference*, en ACSW ’17. New York, NY, USA: Association for Computing Machinery, 2017. doi: 10.1145/3014812.3014820.

[9] T. Guarda, W. Orozco, M. F. Augusto, G. Morillo, S. A. Navarrete, y F. M. Pinto, «Penetration Testing on Virtual Environments», en *Proceedings of the 4th International Conference on Information and Network Security*, en ICINS ’16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 9-12. doi: 10.1145/3026724.3026728.

[10] H. M. Z. A. Shebli y B. D. Beheshti, «A study on penetration testing process and tools», en *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2018, pp. 1-7. doi: 10.1109/LISAT.2018.8378035.

[11]I. U. Haq y T. A. Khan, «Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review», *IEEE Access*, vol. 9, pp. 87806-87825, 2021, doi: 10.1109/ACCESS.2021.3088229.

[12] M. Battaglioni, G. Rafaiani, F. Chiaraluce, y M. Baldi, «MAGIC: A Method for Assessing Cyber Incidents Occurrence», *IEEE Access*, vol. 10, pp. 73458-73473, 2022, doi: 10.1109/ACCESS.2022.3189777.

GLOSARIO

Análisis de Vulnerabilidades: Proceso de identificación, cuantificación y priorización de vulnerabilidades en un sistema, con el objetivo de mitigar posibles riesgos de seguridad.

APT (Amenaza Persistente Avanzada): Tipo de ataque cibernético en el que un intruso se infiltra en una red y permanece sin ser detectado durante un largo período de tiempo, generalmente para robar datos o espiar.

Autenticación Multifactor (MFA): Método de autenticación que requiere más de un factor de verificación, como una contraseña y un código enviado a un dispositivo móvil, para conceder acceso a un sistema.

Backdoor: Método para eludir la autenticación normal en un sistema, frecuentemente dejado por desarrolladores o introducido por atacantes para obtener acceso futuro.

Cifrado: Proceso de convertir datos legibles en un código para evitar el acceso no autorizado, asegurando la confidencialidad y la integridad de la información.

DDoS (Denegación de Servicio Distribuida): Ataque en el que múltiples sistemas comprometidos, a menudo infectados con “malware”, se utilizan para inundar un sistema objetivo con tráfico, causando una Denegación de Servicio (DoS).

Firewall: Sistema de seguridad de red que monitorea y controla el tráfico de red

entrante y saliente según políticas de seguridad preestablecidas, protegiendo así la red interna de accesos no autorizados.

Hacking Ético: Práctica de utilizar habilidades de hacking con el permiso del propietario del sistema, con el objetivo de identificar y solucionar vulnerabilidades de seguridad.

IDS (Sistema de Detección de Intrusos): Dispositivo o software que monitorea las actividades de una red o sistema en busca de actividades maliciosas o violaciones de políticas, generando alertas para los administradores de seguridad.

Penetration Testing (Pruebas de Penetración): Simulación de ataques cibernéticos contra un sistema informático para evaluar la seguridad del sistema y detectar vulnerabilidades que podrían ser explotadas por atacantes.

Phishing: Técnica de ingeniería social utilizada para obtener información confidencial, como contraseñas y datos de tarjetas de crédito, mediante el engaño y la suplantación de identidad.

SIEM (Gestión de Información y Eventos de Seguridad): Sistema que proporciona análisis en tiempo real de alertas de seguridad generadas por aplicaciones y hardware de red, centralizando la gestión de incidentes de seguridad.

VPN (Red Privada Virtual): Tecnología que crea una conexión segura y cifrada sobre una red menos segura, como Internet, permitiendo a los usuarios acceder a recursos de manera segura desde ubicaciones remotas.

Vulnerabilidad: Debilidad en un sistema de información que puede ser explotada por amenazas para obtener acceso no autorizado a datos o causar daños al sistema.

WAF (Firewall de Aplicaciones Web): Dispositivo o software diseñado para proteger aplicaciones web al filtrar y monitorear el tráfico HTTP entre una aplicación web y el Internet.

Footprinting: Proceso de recopilación de información sobre un sistema, red u organización para identificar posibles vulnerabilidades antes de realizar un ataque o prueba de penetración.

ANEXOS

Anexo A: Valoración de los activos

VALORACIÓN DE ACTIVOS DE INFORMACIÓN								
N°	**CÓDIGO**	**TIPO ACTIVO**	**DESCRIPCIÓN**	**RESPONSABLE**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**VALORACION**
1	HW01	HW	Servidor de desarrollo	Jefe de TI	X	X	X	MA
2	HW02	HW	Servidor de desarrollo	Jefe de TI	X	X	X	MA
3	HW03	HW	Servidor de desarrollo	Jefe de TI	X	X	X	MA
4	HW04	HW	Switch Tplink interno 24 puertos	Jefe de TI			X	M
5	HW05	HW	Router inalámbrico del ISP	Jefe de TI	X	X	X	MA
6	HW06	HW	Router VPN	Jefe de TI	X	X	X	M
7	HW07	HW	Router WIFI	Jefe de TI	X	X	X	M
8	HW07	HW	Patch panel	Jefe de TI			X	B
9	S01	S	SVN (Sistema control de versión)	Jefe de TI	X	X	X	A
10	S02	S	Team City (Generador de versión)	Jefe de TI	X	X	X	A
11	S03	S	Microsoft SQL server	Jefe de TI	X	X	X	A
12	S04	S	Servicio de escritorio remoto	Jefe de TI	X	X	X	A
13	SW01	SW	Visual Studio	Jefe de TI		X	X	B
14	SW02	SW	Microsoft SQL Server Management	Jefe de TI	X	X	X	A
15	SW03	SW	Notepad++	Jefe de TI			X	B

Anexo B: Plan de acción

Fase	Objetivo	Acciones	Responsables	Herramientas
Asignar Controles a los Riesgos				
Identificación y Clasificación de Activos	Identificar y clasificar activos	• - Inventariar hardware, software y servicios. • - Clasificar activos por criticidad: alta, media, baja.	Equipo de TI	CMDB, hojas de cálculo
Evaluación de Vulnerabilidades	Identificar vulnerabilidades	• - Escanear con Nessus y OpenVAS. • - Realizar pruebas de penetración con Metasploit, Nmap, Burp Suite. • - Documentar y clasificar vulnerabilidades.	Equipo de Seguridad Informática	Nessus, OpenVAS, Metasploit, Nmap, Burp Suite
Asignación de Controles	Mitigar vulnerabilidades	• - Seleccionar controles de ISO/IEC 27001. • - Implementar parches, actualizaciones, configuraciones seguras. • - Establecer políticas y procedimientos de seguridad.	Equipo de Seguridad Informática	ISO/IEC 27001, políticas de seguridad, procedimientos operativos
Selección de Soluciones Contramedidas, Tiempos y Costos				
Desarrollo de un Plan de Remediación	Crear un plan de remediación	• - Priorizar vulnerabilidades. • - Asignar recursos y responsables. • - Establecer cronograma.	Gerente de TI, Equipo de Seguridad Informática	Herramientas de gestión de proyectos (Microsoft Project, JIRA)
Implementación de Medidas Correctivas	Implementar soluciones técnicas y administrativas	• - Aplicar parches y actualizaciones. • - Configurar firewalls, IDS/IPS. • - Mejorar configuraciones de acceso y autenticación.	Equipo de TI, Equipo de Seguridad Informática	Sistemas de gestión de parches, firewalls, IDS/IPS
Evaluación de Costos	Analizar costo y viabilidad	• - Estimar costos de medidas. • - Evaluar retorno de inversión. • - Aprobar presupuesto.	Gerente de TI, CFO	Hojas de cálculo, software de contabilidad
Implementación de Controles y Validación				
Monitoreo y Auditoría	Asegurar funcionamiento de controles	• - Configurar SIEM. • - Realizar auditorías periódicas. • - Documentar y ajustar controles.	Equipo de Seguridad Informática, Auditores Internos	SIEM, herramientas de auditoría
Pruebas de Penetración Post-Remediación	Validar efectividad de medidas correctivas	• - Realizar nuevas pruebas de penetración. • - Identificar nuevas vulnerabilidades. • - Ajustar medidas correctivas.	Equipo de Seguridad Informática	Metasploit, Nmap, Burp Suite
Capacitación y Concientización				

Programas de Capacitación	Aumentar conciencia de seguridad	• - Desarrollar y realizar programas de capacitación. • - Organizar talleres y seminarios. • - Evaluar conocimiento adquirido.	Recursos Humanos, Equipo de Seguridad Informática	Plataformas de e-learning, materiales de capacitación
Políticas de Seguridad	Establecer y reforzar políticas de seguridad	• - Redactar y distribuir políticas. • - Implementar procedimientos de manejo seguro de información. • - Monitorear y ajustar cumplimiento de políticas.	Equipo de Seguridad Informática, Gerente de TI	Documentación de políticas, software de gestión de cumplimiento
Monitoreo Continuo y Mejora Continua				
Monitoreo Continuo	Detectar y responder a incidentes en tiempo real	• - Implementar SIEM y IDS/IPS. • - Configurar alertas. • - Establecer equipo de respuesta a incidentes.	Equipo de Seguridad Informática	SIEM, IDS/IPS
Revisión y Actualización del Plan de Seguridad	Mantener plan de seguridad actualizado	• - Revisar plan de seguridad cada 6 meses. • - Incorporar lecciones aprendidas. • - Actualizar plan según cambios en TI y nuevas amenazas.	Equipo de Seguridad Informática, Gerente de TI	Documentación de plan de seguridad, revisiones internas

Anexo C: Footprinting